JUSTIÇA & CIDADANIA®

ISSN 1807-779X
Edição 195 - Novembro de 2016
R$ 16,90

MINISTRO RICARDO VILLAS BÔAS CUEVA, DO STJ

A INSUFICIENTE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Editorial: Imprensa Livre

A insuficiente proteção de dados pessoais no Brasil

Ricardo Villas Bôas Cueva
Ministro do STJ
Membro do Conselho Editorial

A coleta, o processamento e a utilização de dados pessoais tendem hoje a alcançar todos os aspectos da vida, graças ao barateamento incessante da informática e do armazenamento de dados. Governos e empresas criam rotineiramente perfis de personalidade que permitem classificar e discriminar os indivíduos consoante seus hábitos, características biológicas, preferências e convicções, em flagrante ameaça não só à privacidade, mas também à própria dignidade humana.

Ampliou-se, por isso, em quase todo o mundo, o campo de proteção dos dados pessoais, mediante legislação específica e o reconhecimento, em muitos países, do direito fundamental à autodeterminação informativa, que faculta ao indivíduo decidir por si só sobre a exibição e o uso de seus dados pessoais. A União Europeia reconheceu-o como direito fundamental em 2000, após países como Portugal e Alemanha terem-no feito nas décadas de 1970 e 1980, respectivamente.

No Brasil, a Constituição Federal protege a intimidade e a vida privada, assim como o sigilo da comunicação de dados. Há também regras legais específicas para a proteção de dados pessoais de consumidores em bancos de dados. Mas não há legislação que discipline toda a matéria de forma unificada e consentânea com os princípios internacionalmente aceitos. Antes de discutirmos a necessidade de um novo marco legal, examinaremos a evolução do conceito de privacidade.

Da privacidade à autodeterminação informativa

O direito à privacidade foi pioneiramente delineado em artigo publicado em 1890 por Samuel Warren e Louis Brandeis, no qual se identificou o direito a ser deixado só (*right to be let alone*), oponível a terceiros, tendo em vista as crescentes ameaças à personalidade humana decorrentes da então incipiente massificação da mídia e do abuso da imagem e de informações pessoais. Com base em precedentes da *common law* sobre ilícitos contra a honra e sobre violações ao direito de propriedade, os autores enunciaram os elementos constitutivos do direito à privacidade, que foi reconhecido na Declaração Universal dos Direitos do Homem (art. 12) e nos ordenamentos jurídicos da maioria dos países.[1]

O rápido desenvolvimento da informática, contudo, multiplicou as possibilidades de invasão da intimidade. A ubiquidade dos meios eletrônicos de coleta e troca de informações permite que se recolham informações virtualmente sobre todas as atividades cotidianas, a fim de organizá-las em categorias de comportamento, de preferências, de crenças, de consumo, entre outras, e assim traçar perfis de personalidade voltados para o exercício de alguma modalidade de controle social, político, econômico ou mesmo existencial sobre os indivíduos. A obtenção e a disseminação massificada e praticamente instantânea dessas informações, cujo conteúdo nem sempre constitui um segredo nem caracteriza uma invasão de privacidade, no sentido clássico que se atribui a este direito, põem em xeque


Foto: Ascom/STJ

a efetividade da tutela jurídica da vida privada, pois os indivíduos são despojados do direito de participar e de algum modo controlar as informações que sobre eles são produzidas e divulgadas, e evidenciam uma crise na própria noção de intimidade.[2]

Na década de 1970, surgem as normas de proteção de dados pessoais de primeira geração, como a lei do *Land* alemão de Hessen (1970), a lei de dados da Suécia (1973), o estatuto de proteção de dados do *Land* alemão de Rheinland-Pfalz (1974) e lei federal de proteção de dados da Alemanha (1977). Nos EUA, foi editado, em 1970, o *Fair Credit Reporting Act* e, em 1974, o *Privacy Act*. Em 1976, Portugal foi o primeiro país a estabelecer em sua constituição o direito fundamental à autodeterminação informativa (art. 35).

Em 1983, a Corte Constitucional da República Federal da Alemanha, em julgamento de reclamação acerca da inconstitucionalidade da lei do recenseamento (*Volkszählungsgesetz*), reconheceu a existência de um direito fundamental à autodeterminação informativa a partir dos direitos fundamentais à dignidade humana e ao livre desenvolvimento da personalidade (arts. 1, I, e 2, I, da lei fundamental alemã). A partir dessa decisão passou-se a compreender a proteção à autodeterminação informativa como fenômeno não apenas privado, mas também coletivo, já que, em certas circunstâncias, os danos decorrentes da violação desse direito podem ser caracterizados como difusos, a exigir mecanismos jurídicos de tutela coletiva. Além disso, o direito à privacidade deixa de ter conteúdo apenas negativo – a capacidade de excluir terceiros de informações pessoais – e ganha conteúdo positivo – a liberdade de o indivíduo decidir como, quando e onde seus dados pessoais podem circular. Por fim, em virtude do desenvolvimento tecnológico, que enseja inúmeras oportunidades de discriminação do indivíduo pelo Estado e por agentes econômicos, o novo conceito de privacidade passa a associar-se também ao direito fundamental à igualdade.[3]

Por outro lado, como os direitos fundamentais irradiam efeitos mediatos, ou horizontais, para as relações interpessoais entre entes privados, pode haver conflito ou colisão com outros direitos fundamentais, como o direito à propriedade, a liberdade de contratar ou a liberdade de exercício de trabalho ou profissão. Em um juízo de ponderação, seria possível concluir que os empregadores e os bancos, por exemplo, são legitimados a conhecer informações detalhadas, respectivamente, sobre candidatos a empregos ou empréstimos. Se, contudo, as relações entre os entes privados forem de tal modo assimétricas que tornem impossível o uso da ponderação, cabe ao legislador desenhar modelos de regras aptos a solucionar adequadamente o conflito de interesses.[4]

Em 2000, a Carta dos Direitos Fundamentais da União Europeia definiu, em seu art. 8º, que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Além disso, tais dados "devem ser objeto de um tratamento leal, para fins específicos e com consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei", sendo certo que "todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação". Por fim, o cumprimento dessas regras "fica sujeito à fiscalização por parte de uma autoridade independente".

Na União Europeia, particularmente relevante para a consolidação da tutela dos dados pessoais foi a Diretiva 95/46, hoje substituída pelo Novo Regulamento Geral de Proteção de Dados, publicado em 4 de maio de 2016, que unifica o direito europeu sobre a matéria, aplicando-se diretamente a todos os Estados-membros. Entre várias inovações, o regulamento impõe multas que podem chegar a 4% do faturamento das empresas ou a €20 milhões e introduz o dever de *accountability*, a realização de análises de impacto sobre a privacidade e a notificação obrigatória às autoridades de proteção de dados em caso de vazamento. O diploma define, ainda, novos direitos, como a portabilidade de dados, o direito ao esquecimento e o direito de se opor à criação de perfil informacional.

Relevantes, ainda, são as diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), as quais definem como princípios básicos da proteção de dados pessoais: a) o princípio da limitação da coleta, que impõe seja ela feita por meios lícitos e, sempre que possível, com o conhecimento ou o consentimento do titular dos dados; b) o princípio da qualidade dos dados, que exige sejam os dados pessoais relevantes para as finalidades para as quais são usados, e que sejam precisos, completos e atualizados; c) o princípio da finalidade, que pressupõe correlação entre o uso dos dados e a finalidade especificada quando de sua coleta; d) o princípio da limitação do uso, que veda a divulgação ou utilização de dados pessoais para finalidade diversa daquela especificada quando da coleta, exceto se houver anuência do titular ou autorização legal; e) o princípio da segurança, que impõe a adoção dos mecanismos necessários a impedir a perda, a destruição, a modificação, a divulgação ou o acesso não autorizado de dados pessoais; f) o princípio da transparência, que supõe a publicidade da existência do banco de dados, de sua natureza e de seu propósito, bem como da identidade e da localização de seu controlador; g) o princípio da participação individual, que confere ao indivíduo o direito de ser informado sobre a existência de dados a seu respeito, bem como de contestá-los perante o controlador do banco de dados e, sendo tal pretensão acolhida, eliminá-los, retificá-los, completá-los ou emendá-los e, h) o princípio da responsabilidade do controlador do banco de dados pelo respeito aos princípios precedentes.[5]

Para Canotilho, o direito ao conhecimento dos dados pessoais informatizados desdobra-se em vários direitos: "(a) o direito de acesso, ou seja, o direito de conhecer os dados constantes de registros informáticos, quaisquer que eles sejam (públicos ou privados); (b) o direito ao conhecimento da identidade dos responsáveis, bem como o direito aos esclarecimentos sobre a finalidade dos dados; (c) o direito de contestação, ou seja, direito à rectificação dos dados e sobre identidade e endereço do responsável; (d) o direito de actualização (cujo escopo fundamental é a correcção do conteúdo dos dados em caso de desactualização); (e) finalmente, o direito à eliminação dos dados cujo registro é interdito".[6]

O direito à proteção dos dados pessoais, que nasce como direito de defesa perante o Estado, hoje tem alcance muito maior. Os milhares de registros eletrônicos gerados em catracas automatizadas, pedágios eletrônicos, câmeras, aparelhos de GPS, eletrodomésticos (a "internet das coisas"), bem como inúmeras outras transações diariamente mediadas pela informática com técnicas avançadas de análise ("big data", por exemplo), deixam claro que o tratamento desarrazoado de dados pessoais pode fomentar a criação de pequenos Leviatãs, cujo potencial ofensivo à vida privada e à dignidade humana pode se igualar ou até mesmo exceder aquele representado pelo Estado.

A proteção dos dados pessoais no Brasil

O *habeas data* foi saudado, em 1988, como importante inovação. Em 1991, ao julgar o Recurso Ordinário em *Habeas Data*, decidiu o Supremo Tribunal Federal que "o *habeas data* configura remédio jurídico-processual, de natureza constitucional, que se destina a garantir, em favor da pessoa interessada, o exercício de pretensão jurídica discernível em seu tríplice aspecto: (a) direito de acesso aos registros; (b) direito de retificação dos registros; e (c) direito de complementação dos registros" (RHD 22-8/DF, rel. para o acórdão Min. Celso de Mello). Ficou assentado que o *habeas data* destina-se a proteger direitos materialmente assegurados na Constituição. Mas, tanto esse entendimento como a disciplina legal do instituto, que só veio à luz em 1997, são invariavelmente criticados em doutrina por seu viés formalista e por sua ineficácia. Luis Alberto Barroso, por exemplo, atribui-lhe valia "essencialmente simbólica", enquanto Dalmo Dallari refere-se a "uma ação voltada para o passado".[7]

Ministro Ricardo Villas Bôas Cueva

Foto: Ascom/STJ

Outra relevante inovação da Constituição de 1988 foi a tutela do sigilo de dados, cujo restrito âmbito de aplicação também tem sido objeto de polêmica. O STF, ao julgar o HC 83.168-1, rel. Min. Sepúlveda Pertence, reafirmou seu entendimento de que o inciso XII do art. 5º da Constituição protege a comunicação de dados, e não os dados em si mesmos. Tal interpretação tem sido criticada por dificultar o reconhecimento do direito fundamental à proteção de dados pessoais.[8]

Por outro lado, o Superior Tribunal de Justiça, ao apreciar a proteção de dados pessoais sob a ótica legislação consumerista, tem se orientado no sentido do reconhecimento de um amplo direito à privacidade. No REsp nº 22.337/RS, rel. Min. Ruy Rosado de Aguiar, no qual se pacificou o entendimento de que sobre os cadastros negativos de devedores incide o disposto no art. 43, § 1º, do CDC, seja no que toca à limitação temporal dos registros negativos, seja no que tange à verdade da informação registrada, houve expressa remissão à matriz constitucional da proteção da intimidade e da vida privada (art. 5º, X, da CF). No REsp nº 1.168.547/RJ, rel. Min. Luiz Felipe Salomão, foi reconhecida a existência de um novo conceito de privacidade, bem como a necessidade de consentimento do interessado para a divulgação de informação pessoal a seu respeito. No REsp 306.570, rel. Min. Eliana Calmon, reconheceu-se que "o contribuinte ou o titular da conta bancária tem direito à privacidade em relação aos seus dados pessoais". Por fim, no REsp 1.419.697, rel. Min. Paulo Sanseverino, sobre as demandas nas quais se postulava danos morais em decorrência da utilização de sistemas de avaliação de crédito (*credit scoring*), decidiu-se, em caráter repetitivo, que "na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei nº 12.414/2011".

A Lei nº 12.414, de 9 de junho de 2011, que trata do cadastro positivo, ampliou o alcance das normas atinentes aos bancos de dados e aos cadastros de consumidores, pois além do direito de acesso e do direito à correção da informação, já previstos no art. 43 do CDC, expressamente incluiu entre os direitos do cadastrado: o direito a obter o cancelamento do cadastro quando solicitado (art. 5º, I); o direito a conhecer os principais elementos e critérios considerados para a análise de risco (art. 5º, IV); o direito a ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento (art. 5º, V); o direito de solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizado (art. 5º, VI), e o direito a ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados (art. 5º, VII). Com isso, nosso ordenamento passou a contar com proteção de dados pessoais – ainda que somente para efeito de cadastro positivo de crédito – mais afinada com os princípios internacionalmente aceitos.

> "O STF, ao julgar o HC 83.168-1, rel. Min. Sepúlveda Pertence, reafirmou seu entendimento de que o inciso XII do art. 5º da Constituição protege a comunicação de dados, e não os dados em si mesmos. Tal interpretação tem sido criticada por dificultar o reconhecimento do direito fundamental à proteção de dados pessoais."

A Lei nº 12.527/2011, ao disciplinar o acesso a informações públicas, inclusive as de caráter pessoal, sob a égide de princípios aplicáveis internacionalmente ao tratamento de informações, prevê a designação de responsável pelo cumprimento da lei de acesso a informações, o que pode ser o primeiro estágio no sentido da criação de um tipo de autoridade independente encarregada de supervisionar não somente o acesso a informações públicas (e privadas), como, num futuro que se espera não muito distante, toda a atividade de proteção dos dados pessoais e da autodeterminação informativa.

Necessidade de um marco legal da proteção de dados pessoais

Como se viu, a Constituição Federal tutela a intimidade e a vida privada, o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, X e XII) e assegura a concessão de *habeas data* (art. 5º, LXIX e LXXII). Além disso, o Código de Defesa do Consumidor contém regras específicas sobre bancos de dados e cadastros de consumidores, a Lei nº 12.414/2011 disciplina o cadastro positivo e a Lei nº 12.527/2011 regula o acesso a informações públicas. Há, portanto, alguma proteção aos dados pessoais. Mas a limitada aplicabilidade da lei consumerista, neste aspecto, a jurisprudência restritiva do Supremo Tribunal Federal acerca do *habeas data* e do sigilo de dados, bem como a ausência de princípios claros a nortear a proteção de dados pessoais indicam que ainda há muito a fazer nos planos doutrinário, legislativo e jurisprudencial para que a proteção de dados pessoais se torne efetiva no Brasil.

A edição de lei nacional de proteção dos dados pessoais é essencial para suprir as omissões hoje existentes e garantir um nível adequado de proteção. Já se encontra em tramitação na Câmara dos Deputados o Projeto de Lei nº 5.276/2016, do Executivo, que resultou de consulta pública realizada no Ministério da Justiça, no qual são definidos os dados pessoais passíveis de proteção, os princípios aplicáveis a seu tratamento, bem como os direitos básicos de seus titulares (ARCO: acesso, retificação, cancelamento e oposição). O projeto define também os agentes responsáveis pelo tratamento de dados, as medidas de segurança exigíveis, além de fixar as sanções administrativas a serem aplicadas pelo órgão competente pela fiscalização da lei, o qual não é indicado expressamente, embora tenha suas competências definidas. Além disso, cria-se o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Paralelamente, tramita no Senado o Projeto de Lei nº 330/ 2013, com características muito semelhantes. Seu autor, o Senador Aloysio Nunes Ferreira, aponta a necessidade de previsão de uma autoridade central de proteção de dados pessoais. É imperioso que o Congresso se disponha a apreciar com presteza quaisquer dos dois projetos de lei.

Notas

[1] Warren, Samuel; Brandeis, Louis, "The right to privacy", Harvard Law Review, vol. IV, nº 5, dezembro de 1890, p. 193 e ss.

[2] Hassemer, Winfried; Sanchéz, Alfredo Chirino, *El Derecho a la Autodeterminación Informativa y los Retos del Procesamiento Automatizado de Datos Personales*, Buenos Aires, Editores del Puerto, 1997.

[3] Mendes, Laura Schertel, "O direito fundamental à proteção de dados pessoais" in Revista de Direito do Consumidor, vol. 79, jul-2011, pp. 45 e ss.

[4] Cf. Tinnefeld, Marie-Thres, *Einführung in das Datenschutzrecht*, Munique, Ed. R. Oldenbourg, 1994, p. 37.

[5] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" in HTTP:/WWW.oecd.org, consultado em 16/2/2012.

[6] Canotilho, J.J. Gomes, *Constituição da República Portuguesa anotada*, vol. 1, São Paulo, RT, 1ª Ed., 2007, p. 550 ss.

[7] Cf., respectivamente, Barroso, Luis Alberto, "Viagem redonda: habeas data, direitos constitucionais e provas ilícitas" in Wambier, Teresa Arruda Alvim (coord.), *Habeas data*, São Paulo, RT, 1998, p. 212 e Dallari, Dalmo de Abreu, "O habeas data no sistema jurídico brasileiro" in Revista de La Facultad de Derecho de La Pontifícia Universidad Católica del Perú, nº 51, 1997, p. 100.

<?> Doneda, Danilo, "A proteção dos dados pessoais como um direito fundamental" in Espaço Jurídico, Ed. Unoesc, v. 12, nº 2, jul/dez 2011, pp.91-108.